Le scandale Cambridge Analytica contextualisé: le capital de plateforme, la surveillance et les données comme nouvelle « marchandise fictive »

The Cambridge Analytica Scandal Contextualized: Platform Capital, Surveillance, and Data as a New 'Fictitious Commodity'

Ivan Manokha

Édition électronique

URL : <http://journals.openedition.org/conflits/19779>

DOI : 10.4000/conflits.19779

ISSN : 1777-5345

Éditeur :

CCLS - Centre d'études sur les conflits liberté et sécurité, L'Harmattan

Édition imprimée

Date de publication : 20 juillet 2018

Pagination : 39-59

ISBN : 978-2-343-15504-3

ISSN : 1157-996X

Référence électronique

Ivan Manokha, « Le scandale Cambridge Analytica contextualisé: le capital de plateforme, la surveillance et les données comme nouvelle « marchandise fictive » », *Cultures & Conflits* [En ligne], 109 | printemps 2018, mis en ligne le 20 juillet 2020, consulté le 30 mars 2021. URL : <http://journals.openedition.org/conflits/19779> ; DOI : <https://doi.org/10.4000/conflits.19779>

Le scandale Cambridge Analytica contextualisé : le capital de plateforme, la surveillance et les données comme nouvelle « marchandise fictive »

Ivan MANOKHA

Ivan Manokha occupe le poste de Departmental Lecturer au sein du département du développement international à l'Université d'Oxford. Ses recherches portent sur les questions de pouvoir et d'obéissance dans l'économie politique internationale, notamment dans le contexte du développement des nouvelles technologies de surveillance, ainsi que de la montée en puissance des plateformes numériques dont les revenus et l'influence croissante sont basés sur la collecte permanente des données et leur monétisation.

Le 17 mars 2018, l'*Observer* de Londres ¹ et le *New York Times* ² ont révélé que Cambridge Analytica, société de conseil en stratégie basée à Londres, avait recueilli des données personnelles issues des profils Facebook de plus de cinquante millions d'utilisateurs sans leur consentement, le chiffre ayant ensuite été réévalué à quatre-vingt-sept millions ³. La collecte de données a été effectuée via une application de quiz « thisisyourdigitallife », créée pour Facebook par Aleksandr Kogan. Ce psychologue de l'université de Cambridge a eu accès aux données personnelles de deux cent soixante-dix mille membres de Facebook qui avaient accepté de se soumettre à un test de personnalité pour lequel ils ont été rémunérés par son entreprise, Global Science Research. Comme l'a expliqué Christopher Wylie, expert en données canadien et ancien employé de Cambridge Analytica ⁴, cette application per-

-
1. Cadwalladr C. et E. Graham-Harrison, « Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach », *The Observer*, 17 mars 2018.
 2. Rosenberg M., Confessore N. et E. Cadwalladr, « How Trump Consultants Exploited the Facebook Data of Millions », *The New York Times*, 17 mars 2018.
 3. Solon O., « Facebook Says Cambridge Analytica May Have Gained 37m More Users' Data », *The Guardian*, 4 avril 2018.
 4. « Cambridge Analytica Whistleblower: 'We Spent \$1m Harvesting Millions of Facebook Profiles' », *The Guardian*, 17 mars 2018.

mettait de collecter différents types de données personnelles des utilisateurs (les contenus consultés et « likés », et même les messages publiés) ; de plus, elle donnait accès aux informations figurant sur les profils des amis de chacun des utilisateurs qui avaient accepté de passer ce test, ce qui explique que tant d'utilisateurs aient été affectés. Ces données étaient ensuite transmises à Cambridge Analytica, recrutée par l'équipe de campagne de Donald Trump en juin 2016, qui les aurait utilisées pour cibler les électeurs américains en leur adressant des messages politiques personnalisés « visant leurs démons intérieurs ⁵ ».

Les gouvernements ont rapidement réagi à ces révélations et à l'indignation massive qu'elles ont suscitée ⁶. Le 19 mars 2018, Antonio Tajani, président du Parlement européen, a déclaré dans un message Twitter que l'utilisation abusive des données des utilisateurs de Facebook constituait « une violation inacceptable des droits [des] citoyens en matière de vie privée ⁷ » et a promis une enquête de l'Union européenne (UE). Le 21 mars, des procureurs brésiliens ont ouvert une enquête sur Cambridge Analytica ⁸, suivis le lendemain par le ministre de la Justice israélien dénonçant des violations potentielles des informations personnelles des citoyens israéliens par Facebook ⁹. Le 27 mars, Christopher Wylie a été auditionné en tant que témoin par la commission du numérique, des médias et des sports du Parlement britannique et le 10 avril 2018, le PDG de Facebook, Mark Zuckerberg, a témoigné devant le Congrès des États-Unis. Enfin, le 2 mai 2018, quarante-six jours après le début du scandale, sous la pression croissante de différents acteurs gouvernementaux et non gouvernementaux, Cambridge Analytica, ainsi que sa maison mère SCL, ont annoncé leur fermeture.

Aussi choquante soit-elle, l'affaire Cambridge Analytica n'est qu'un exemple – d'ailleurs relativement mineur – des pratiques en matière de collecte

5. Cadwalladr C. et E. Graham-Harrison, « Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach », *op. cit.*
6. On peut noter que la collecte massive des données par Cambridge Analytica, ainsi que leur utilisation dans les campagnes électorales dans différents pays (y compris dans le référendum sur le Brexit au Royaume-Uni et les élections présidentielles américaines) avaient déjà fait l'objet de quelques enquêtes journalistiques (voir, par exemple, Grassegger H. et M. Krogerus M., « The Data That Turned the World Upside Down », *Motherboard*, 28 janvier 2017, en ligne sur https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win, consulté le 13/05/2018). Toutefois, elles n'avaient pas suscité un grand écho dans le public. Il est probable que ce manque de retentissement s'explique par le fait que les enquêtes précédentes, à la différence de celles de l'*Observer* et du *New York Times*, n'évoquaient que des moyens de collecte des données qui n'étaient pas perçus comme illégitimes – tels que la consultation des sources publiques (par exemple, des cadastres) ou l'utilisation des données issues des courtiers en données (tels que Acxiom or Experian).
7. Tajani A. Message posté sur Tweeter le 19 mars 2018, en ligne sur https://twitter.com/EP_President/status/97568324077453569, consulté le 19/03/2018.
8. Brito R., « Brazil Prosecutors Open Investigation into Cambridge Analytica », Reuters, 21 mars 2018.
9. Wootliff R., « Israel to Probe Facebook over Cambridge Analytica Data Breach », *The Times of Israel*, 22 mars 2018.

de données et de violations de confidentialité, effectuées de manière systématique et quotidienne par différents acteurs, et notamment les plateformes numériques. À cet égard, lorsque l'on accède aux deux articles de l'*Observer* et du *New York Times* qui l'ont dévoilée, ce sont respectivement soixante-quinze et soixante-et-un sites tiers qui reçoivent des informations issues du navigateur de l'utilisateur ¹⁰. Il est par conséquent nécessaire d'examiner les conditions qui rendent possibles de tels vols de données et d'analyser plus globalement la collecte de données et leur monétisation en tant qu'activité génératrice de revenus, qui s'est normalisée et fait désormais partie intégrante de notre système socio-économique.

Quelques études récentes ont abordé cette question en y associant l'expression de « capitalisme de surveillance », employée pour la première fois par Foster et McChesney ¹¹ et développée plus tard par d'autres auteurs, et notamment Shoshana Zuboff ¹². Cependant, la portée de ces travaux reste limitée. En effet, de l'aveu même de cette dernière, l'étude du « capitalisme de surveillance », qu'elle définit comme un « nouveau capitalisme », n'a pas encore été délimitée ou théorisée ¹³. D'autre part, les analyses existantes se caractérisent par un certain nombre de faiblesses. Tout d'abord, les évolutions identifiées – l'accroissement de la quantité des données collectées par les acteurs du secteur privé au sujet des clients, utilisateurs, marchés, etc. – pour étayer l'affirmation selon laquelle nous vivons désormais dans l'ère du « capitalisme de surveillance », sont loin d'être récentes et sont uniquement d'ordre quantitatif. Ainsi, Shoshana Zuboff soutient par exemple que le « capitalisme de surveillance » a émergé « au cours de la dernière décennie ¹⁴ ». Or les sondages auprès des consommateurs, les études de marché, les cartes de fidélité et la publicité existent depuis longtemps et ont toujours eu pour visée d'influencer le comportement et les choix du consommateur. Comme l'observaient déjà Baran et Sweezy ¹⁵ en 1966, les politiques fordistes de salaires élevés visaient à inciter les travailleurs à dépenser leur argent dans l'achat de marchandises (souvent superflues) grâce à la publicité, qui a joué un rôle central dans le développement de la « culture de consommation » au cours des années 1950, et au marketing, qui est rapidement devenu un système complexe de surveillance et de ciblage des consommateurs. Des critiques similaires peuvent

10. L'analyse des deux pages web a été effectuée par l'auteur le 22 avril 2018 à l'aide de l'extension 'Lightbeam' du navigateur Mozilla Firefox.

11. Foster J. et R. McChesney, « Surveillance Capitalism Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age », *Monthly Review*, vol. 66, n° 3, 2014 (version électronique), en ligne sur <https://monthlyreview.org/2014/07/01/surveillance-capitalism/>, consulté le 21/04/2018.

12. Zuboff, S., « Big Other: Surveillance Capitalism and the Prospects of an Information Civilization », *Journal of Information Technology*, vol. 30, 2015, pp. 75-89, et Zuboff, S., « The Secrets of Surveillance Capitalism », *Frankfurter Allgemeine Zeitung*, 5 mars 2016.

13. Zuboff S., « Big Other: Surveillance Capitalism and the Prospects of an Information Civilization », art. cit., pp. 76-77.

14. *Ibid.*, p. 75.

15. Baran P. et P. Sweezy, *Monopoly Capital*, New York, Monthly Review Press, 1966.

être formulées à l'encontre de Foster et McChesney ¹⁶, qui établissent un lien entre l'essor du « capitalisme de surveillance » et « l'hégémonie impérialiste de l'armée américaine et l'accumulation de capital » dans la période d'après-guerre, qui auraient « naturellement entraîné » la création d'ennemis de l'intérieur et leur surveillance subséquente. Selon ces auteurs, l'avènement de la financiarisation dans les années 1980 a conduit le secteur privé (en particulier les banques) à intensifier la collecte de données de leurs clients, ce qui aurait favorisé la consolidation du « capitalisme de surveillance ». Toutefois, la bureaucratie étatique, et les pratiques de surveillance qui en sont inhérentes, constituent l'une des principales caractéristiques de la modernité occidentale ¹⁷ et ne datent évidemment pas de la période d'après-guerre aux États-Unis.

En outre, Shoshana Zuboff affirme que les précédentes phases du capitalisme étaient caractérisées par le « dynamisme de la démocratie de marché ¹⁸ » et que l'avènement du « capitalisme de surveillance » aurait remodelé la « structure du pouvoir, la conformité et la résistance héritées de la société de masse [symbolisée], pendant plus d'un demi-siècle, par le concept de "*Big Brother*". Le pouvoir ne peut plus se résumer à ce symbole totalitaire de commande et de contrôle centralisé. Même le panoptique de Bentham [...] est prosaïque comparé à cette nouvelle architecture ¹⁹ ». Toutefois, il est important de garder à l'esprit que, dans le capitalisme, le marché a toujours été un domaine de contrainte et d'asservissement pour la grande majorité des personnes qui ne possèdent aucun moyen de production, hormis leur « capital humain », et qui doivent vendre leur force de travail contre une rémunération afin d'assurer leur subsistance ²⁰. Par ailleurs, la surveillance a toujours été au cœur du rapport salaire-travail, car les employeurs ont toujours tenté d'ajuster le temps de travail effectif des employés au temps pour lequel ils sont rémunérés (les études de Frederick Taylor en constituent l'une des illustrations les plus connues). Et n'oublions pas que Foucault, dans son analyse de la montée du panoptisme au sein de la société moderne, l'a toujours liée au développement du système capitaliste, dans lequel les prisons s'apparentent à des usines et les usines à des prisons ²¹.

16. Foster J. et R. McChesney, « Surveillance Capitalism Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age », art. cit.

17. Voir, par exemple, Weber M., *Economy and Society*, Volume I, Berkeley, University of California Press, 1978, ainsi que Giddens A., *The Nation-State and Violence: A Contemporary Critique of Historical Materialism*, Volume II, Cambridge, Polity Press, 1985, et Dandeker C., *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*, Cambridge, Polity Press, 1990.

18. Zuboff S., « Big Other: Surveillance Capitalism and the Prospects of an Information Civilization », art. cit., pp. 81-82.

19. *Ibid.*, p. 82.

20. Voir notamment Wood E., *Democracy Against Capitalism: Renewing Historical Materialism*, Cambridge, Cambridge University Press, 1995 ; Wood E., *The Origin of Capitalism*, Londres, Verso, 2002, et Brenner R., « The Origins of Capitalist Development. A Critique of Neo-Smithian Marxism », *New Left Review*, n° 104, 1977, pp. 25-92.

Enfin, aucune de ces études ne traite réellement du fonctionnement du capitalisme et de la manière dont la surveillance contemporaine peut l'avoir affecté. La logique implicite ou explicite des arguments avancés par ceux qui utilisent la notion de « capitalisme de surveillance » peut être synthétisée comme suit : les entreprises recueillent de plus en plus de données et, dans la mesure où celles-ci sont ensuite monétisées – utilisées par les entreprises pour générer du profit – cela signifie que nous avons affaire à un « capitalisme de surveillance ». À titre d'exemple, Priya Kumar, dans son analyse des politiques de confidentialité des entreprises, s'inspire du travail de Zuboff et soutient que « certaines des plus grandes entreprises internet au monde opèrent selon une logique de capitalisme de surveillance ²² ». Selon elle, ceci tient au fait que les entreprises « emploient des techniques avancées d'analyse des données afin [...] d'extraire des revenus issus de la publicité, ce qui transforme les données en ce que Zuboff appelle des "actifs de surveillance" ²³ ». Un argument similaire est formulé par Jacob Silverman dans son analyse de l'impact de la surveillance de la vie privée par les entreprises, lorsqu'il soutient que « la surveillance des informations personnelles et des comportements est devenue l'un des aspects majeurs du capitalisme de surveillance contemporain ²⁴ ». Autrement dit, dans ces travaux, le terme « surveillance » est relié au terme « capitalisme » du simple fait que le premier implique la collecte de données, alors que l'une des caractéristiques du second est la génération de revenus. Comme les entreprises recueillent des données dans l'optique de réaliser du profit, on en déduit que nous avons affaire à un « capitalisme de surveillance » (qui, par ailleurs, reste inexpliqué). Ces travaux n'abordent pas des sujets tels que la part des activités commerciales basées sur les données dans l'activité économique globale, ou la relation entre la collecte des données et leur monétisation et les facteurs de production traditionnels, ou encore l'impact du processus de création de valeur reposant sur les données sur les industries plus conventionnelles.

Dans la phase actuelle du capitalisme, la surveillance joue certes un rôle important dans l'accumulation du capital. Toutefois, les motifs de ce constat diffèrent de ceux avancés par les auteurs susmentionnés. D'une part, les données peuvent être considérées comme une nouvelle « marchandise fictive », à l'instar du travail, de la terre et de la monnaie qui, selon Polanyi, ont été transformés en « marchandises fictives » par la montée du capitalisme ²⁵. D'autre part, le capitalisme d'aujourd'hui se caractérise par l'importance accrue de ce

21. Par exemple, Foucault M., *Surveiller et punir. Naissance de la prison*, Paris, Gallimard, 1975 et Foucault M., « The Eye of Power », in Gordon C. (ed.) *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977*, New York, Pantheon Books, 1980.

22. Kumar P., « Corporate Privacy Policy Changes during PRISM and the Rise of Surveillance Capitalism », *Media and Communication*, vol. 5, n° 1, 2017, p. 68.

23. *Ibid.*, p. 68.

24. *Idem.*

25. Polanyi K., *The Great Transformation: The Political and Economic Origins of Our Time*, New York, Farrar & Rinehart, 1944.

qui est appelé ici le « capital de plateforme », à savoir les plateformes numériques qui opèrent en tant que moyens de production à part entière, utilisant les données en tant qu'unique intrant, (comme le fait par exemple Facebook avec les données utilisateur), ou en tant que moyens auxiliaires de production (lorsqu'elles sont combinées à d'autres intrants tels que les machines, le capital humain, la propriété foncière, etc., comme c'est le cas pour Uber, Airbnb ou industrie 4.0). Il convient de souligner que le capital de plateforme ne devient capital que lorsqu'il est combiné à cette nouvelle « marchandise fictive » qui lui tient lieu de « matière première » principale (ou unique). Pour paraphraser Marx, le capital de plateforme doit rencontrer sur le marché un type de marchandise spécial – les données (en particulier, les données utilisateur) afin de croître et de produire de la valeur. Ainsi, le mode opératoire de ce « capital de plateforme » repose nécessairement sur la collecte permanente des informations relatives aux utilisateurs (et, de plus en plus, relatives aux objets matériels également), le traitement de ces données, l'établissement de profils, le recoupement et enfin l'utilisation de ces données dans le processus de création de valeur.

Tout comme les industries traditionnelles ont besoin de matières premières pour croître, le fonctionnement et la croissance des plateformes dépendent aussi de la matière première qu'elles utilisent, à savoir les données. Leurs activités induisent une nécessité *structurelle* de porter atteinte à la vie privée, qui ne saurait être réduite aux intentions ou actions des acteurs individuels (par exemple, Google, tel qu'analysé par Zuboff, ou Facebook, Amazon ou toute autre plateforme). À cet égard, l'argument développé ici est que nous vivons dans une période marquée par la montée en puissance (et, dans un avenir relativement proche, peut-être même l'hégémonie) du « capital de plateforme » dans le capitalisme mondial. Étant donné que sa capacité à créer de la valeur est tributaire de la surveillance, on peut considérer que la surveillance est la structure même du capital de plateforme.

Pour ce qui est du cas de Cambridge Analytica, il est nécessaire d'aller au-delà de l'étude des mécanismes spécifiques qui ont permis le vol des données (l'application utilisée, la manière dont cette société a obtenu les données des utilisateurs, l'absence de supervision de la part de Facebook, les intérêts de Cambridge Analytica, etc.). Il convient de situer ce cas dans le cadre de l'analyse des conditions structurelles qui rendent possibles de tels événements. Alors que les données deviennent une marchandise et constituent la principale « matière première » du capitalisme de plateforme, la surveillance et les invasions permanentes de la sphère privée sont désormais essentielles au fonctionnement de nombreuses entreprises, notamment les plateformes numériques, ainsi que d'autres entités, à l'instar des courtiers en données (*data brokers*) ou des sociétés de conseil. L'échange de données entre ces acteurs est désormais très répandu. À titre d'exemple, des courtiers en données tels que Acxiom,

Experian ou PeekYou, qui recueillent des données personnelles issues de différentes sources publiques et privées (recensement, fichiers de permis de conduire, rapports de tribunaux, fichiers électoraux, autorités sanitaires, etc.), collaborent avec différentes plateformes (Facebook, Twitter, LinkedIn et autres) afin d'enrichir leurs bases de données et de vendre à ces plateformes des informations qu'elles ne possèdent pas au sujet de leurs utilisateurs. Dans ce contexte, il n'est pas surprenant que différentes entités commerciales (ainsi que des agences gouvernementales telles que les services de sécurité) puissent être intéressées par les données en possession des plateformes (dont le volume est immense) et tentent d'y avoir accès, même de manière dissimulée, comme cela s'est produit dans le cas de Cambridge Analytica, dans celui de la National Security Agency (NSA) révélé par Edward Snowden en 2013 ou, plus récemment, dans le cas de l'entreprise de surveillance israélienne Terrogeance qui a élaboré clandestinement une base de données de reconnaissance faciale ²⁶ constituée de visages « collectés à partir de sources telles que Facebook, YouTube et des forums publics ou privés aux quatre coins de la planète ²⁷ ». Lorsqu'elles sont révélées, ces actions suscitent une forte indignation publique et entraînent souvent la mise en place de mesures spécifiques afin de prévenir de nouveaux vols de données à l'avenir. Toutefois, même si les vols de données par des tiers sont limités (par exemple, grâce à de nouvelles réglementations ou un contrôle renforcé), tant que celles-ci resteront une marchandise et l'intrant principal du capital de plateforme, les invasions de la sphère privée individuelle perdureront. Même si les dispositions légales relatives à la protection et à la confidentialité des données sont renforcées, les plateformes, dont les revenus massifs dépendent des données des utilisateurs, continueront à les contourner, tout simplement parce qu'elles ne peuvent faire autrement. À cet égard, si ceux qui s'indignent de l'action de Cambridge Analytica ne remettent pas en cause toute forme de collecte de données, ils contribueront à renforcer la normalisation des pratiques de surveillance adoptées par le capital de plateforme et ses partenaires et, ce faisant, serviront involontairement leurs intérêts.

L'ascension du capital de plateforme

La dernière décennie a été marquée par la croissance des plateformes numériques et leur hégémonie dans certaines branches de l'économie (la recherche internet et les réseaux sociaux par exemple) et leur importance grandissante dans d'autres (comme le transport urbain). Tout d'abord, que recouvrent exactement les plateformes ? Elles peuvent se définir comme des infrastructures numériques qui mettent en relation les producteurs, les consomma-

26. Fox-Brewster T., « These Ex-Spies Are Harvesting Facebook Photos For A Massive Facial Recognition Database », *Forbes*, 18 avril 2018.

27. Terrogeance, « Biometric Database Enhancement », en ligne sur <https://www.terrogeance.com/capabilities/biometric-database-enhancement/>, consulté le 22/04/2018.

teurs, les prestataires de service, les publicitaires et autres groupes dans un écosystème interactif en permettant l'échange de produits, services ou informations. Le développement des plateformes a été fulgurant : aujourd'hui, les quatre premières entreprises dans la liste des marques les plus valorisées de *Forbes* sont des plateformes, et elles sont onze dans le top vingt ²⁸. La plupart des introductions en bourse et acquisitions récentes concerne des plateformes, de même que la majorité des startups à succès. La liste inclut Apple, Google, Microsoft, Facebook, Twitter, Amazon, eBay, Instagram, YouTube, Twitch, Snapchat, WhatsApp, Waze, Uber, Lyft, Handy, Airbnb, Pinterest, Square, Social Finance, Kickstarter, etc. Bien que la plupart des plateformes soient basées aux États-Unis, elles incarnent un phénomène réellement mondial et jouent un rôle encore plus important dans les pays en voie de développement qui ne possédaient pas d'infrastructures commerciales viables et qui ont saisi l'opportunité offerte par la révolution digitale pour organiser leur industrie autour du cyberspace. En Chine, par exemple, la majorité des entreprises les plus rentables sont des plateformes, notamment Tencent (propriétaire des plateformes de messagerie WeChat et QQ) et Baidu (moteur de recherche) ; Alibaba contrôle 80 % du commerce électronique en Chine par l'intermédiaire de ses plateformes Taobao et Tmall, sa plateforme Alipay étant la plus large en Chine ²⁹.

Si la part des plateformes dans l'indice global S&P 500 n'est pas très importante à l'heure actuelle (inférieure à 5 %), elle devrait, selon les prévisions, constituer la majorité des grandes valorisations du S&P 500 dans les cinq-dix prochaines années, les principaux candidats étant LinkedIn, Twitter, Zillow, GrubHub, Uber, Snapchat, Airbnb, Dropbox et Pinterest, dont les valorisations actuelles dépassent déjà les exigences minimales de capitalisation de l'indice. Et si les tendances actuelles se confirment, les plateformes pourraient représenter 50 % du revenu net du S&P 500 d'ici 25 ans ³⁰.

L'importance des plateformes est également démontrée par le nombre d'utilisateurs – qui se compte souvent en millions, voire en milliards dans certains cas – se connectant régulièrement à leurs différents services basés sur le *cloud*, ainsi que par le large éventail de secteurs dans lesquels elles opèrent désormais. Ainsi, elles jouent désormais un rôle central dans les secteurs-clés suivants : la recherche internet (Google, Yahoo, Bing), les réseaux sociaux (Facebook, LinkedIn, Instagram, Snapchat), les ventes aux enchères et au détail sur internet (eBay, Taobao, Amazon, Alibaba), les services financiers et ressources humaines en ligne (Workday, Upwork, Elance, TaskRabbit), le

28. « The World's Most Valuable Brands: 2017 Ranking », *Forbes Magazine*, 2017, en ligne sur <https://www.forbes.com/powerful-brands/list/>, consulté le 15/04/2018.

29. Moazed A. et N. Johnson, *Modern Monopolies: What It Takes To Dominate The 21st-Century Economy*, New York, St. Martin's Press, 2016.

30. *Idem*.

transport urbain (Uber, Lyft, Zipcar, BlaBlaCar), le tourisme (Kayak, Trivago, Airbnb), les paiements mobiles (Square Order, PayPal, Apple Pay, Google Wallet), le développement de logiciels (App Store d'Apple, Google Play Store, Windows App store) et la santé en ligne (23andMe, PatientsLikeMe, Parkinson mPower). Les solutions basées sur des plateformes commencent également à être adoptées dans des secteurs plus conventionnels tels que la production industrielle (GE, Siemens), l'agriculture (John Deere, Monsanto) et les énergies propres (Sungevity, SolarCity, EnerNOC).

Ces développements ne sont pas passés inaperçus et un grand nombre de néologismes ont été développés dans la littérature académique et non académique afin de conceptualiser ce nouveau phénomène. Toutefois, un examen plus attentif révèle que ces termes et analyses ont tendance à mettre l'accent sur des innovations et nouveautés spécifiques et isolées, plutôt que sur les mutations plus structurelles que subit le capitalisme du fait de l'essor de ces plateformes. Par exemple, ceux qui utilisent le terme désormais très populaire d'« économie de partage » (*sharing economy*) – également « économie de pair à pair » (*peer-to-peer economy*) ou « économie collaborative » (*collaborative economy*) – étudient surtout la consommation collaborative (*collaborative consumption*), la colocation et le troc collaboratif³¹ ; ceux qui examinent la *gig economy* se focalisent essentiellement sur les nouvelles possibilités offertes par les plateformes en vue du recrutement de prestataires indépendants et *freelancers*, à la place d'employés à plein temps, et sur les implications de ce phénomène pour l'emploi³² ; pour finir, les auteurs utilisant le terme « économie à la demande » (*on-demand economy*) ont tendance à mettre en exergue la « commodité de la livraison » proposée par les plateformes aux consommateurs, en particulier dans les secteurs de la restauration, de l'achat et de la livraison d'aliments et du transport, ainsi que les questions relatives au droit du travail³³.

31. Par exemple, Brescia R., « Regulating the Sharing Economy: New and Old Insights into an Oversight Regime for the Peer-to-Peer economy », *Nebraska Law Review*, vol. 95, n° 1, 2016, pp. 88-145 ; Hamari, J., Sjöklint M. et A. Ukkonen, « The Sharing Economy: Why People Participate in Collaborative Consumption », *Journal of the Association for Information Science and Technology*, vol. 67, n° 9, 2016, pp. 2047-2059 ; Taihagh A., « Crowdsourcing, Sharing Economies and Development », *Journal of Developing Societies*, vol. 33, n° 2, 2017, pp. 191-222.
32. Par exemple, Todolí-Signes A., « The End of the Subordinate Worker? Collaborative Economy, On-Demand Economy, Gig Economy, and the Crowdworkers' Need for Protection », *International Journal of Comparative Labour Law and Industrial Relations*, vol. 33, n° 2, 2017, pp. 241-268 ; De Stefano V., « The Rise of the 'Just-in-Time' Workforce: On-Demand Work, Crowd Work and Labour Protection in the "Gig-Economy" », *ILO Conditions of Work and Employment Series*, n° 71, 2016 ; Stewart A. et J. Stanford, « Regulating Work in the Gig Economy: What are the Options? », *The Economic and Labour Relations Review*, vol. 28, n° 3, 2017, pp. 382-401.
33. Par exemple, Heller N., « Is the Gig Economy Working? », *The New Yorker*, 15 mai 2017, en ligne sur <https://www.newyorker.com/magazine/2017/05/15/is-the-gig-economy-working>, consulté le 17/04/2018 ; Natour F., « Respecting Human Rights in the On-Demand Economy: Closing the New Governance Gap », *Business and Human Rights Journal*, vol. 1, n° 2, 2016, pp. 315-320.

Quelques études ont néanmoins tenté d'aller plus loin en analysant ces évolutions comme révélatrices de changements fondamentaux dans l'essence de l'accumulation du capital et dans le capitalisme en tant que système socio-économique. L'un des ouvrages importants en la matière est *Platform Capitalism* de Nick Srnicek ³⁴, dans lequel l'auteur examine la montée des activités de plateforme comme faisant partie intégrante de la trajectoire historique du capitalisme, et établit un lien avec les crises de 1970 et de 2008. Si son travail apporte un ensemble de réflexions sur la nature des activités basées sur les plateformes (et une typologie des plateformes que le présent article utilisera dans la discussion ci-après), son affirmation selon laquelle nous avons affaire aujourd'hui à un « capitalisme de plateforme » est contestable car, comme indiqué précédemment, la part des entreprises et activités basées sur une plateforme dans la production totale, même aux États-Unis, reste relativement marginale (du moins, pour le moment). En outre, il n'aborde pas la transformation essentielle que les plateformes apportent au capitalisme, à savoir, la manière dont ces moyens de connexion deviennent de nouveaux moyens de production.

Srnicek distingue les types de plateforme suivants : plateformes publicitaires, plateformes « *cloud* », plateformes industrielles, plateformes de produit et plateformes de production au plus juste (*lean platforms*) ³⁵. À la lumière de l'argument développé ci-dessus, il serait utile d'établir plutôt une distinction entre les plateformes comme moyens de production à part entière, c'est-à-dire celles qui génèrent des revenus en utilisant les données comme matière première sans s'associer à d'autres facteurs de production, et les plateformes comme moyens de production associés à d'autres facteurs de production pour créer de la valeur. Examinons maintenant ces deux catégories.

Relèvent de la première catégorie ce que Srnicek appelle les « plateformes publicitaires » ainsi que les « plateformes de troc ». Celles-ci tirent la majeure partie de leurs revenus de la publicité ciblée et opèrent, en général, selon le cheminement suivant : elles collectent les données des utilisateurs (et, de plus en plus, celles des objets connectés), puis elles utilisent différents algorithmes pour fabriquer à partir de cette « matière première » des produits vendus aux publicitaires, notamment pour cibler des catégories précises d'utilisateurs triés sur la base de différents critères (leurs goûts, centres d'intérêt, tranches d'âge, activités récréatives, hobbies, etc.). Dans le cas d'espèce, tous les intrants (à l'exception des serveurs), ainsi que les produits finaux, sont immatériels ou basés sur le *cloud* (mis à la disposition des utilisateurs *via* internet par les serveurs des fournisseurs) – il s'agit d'algorithmes, de lignes de code, d'espaces publicitaires pour cibler les profils d'utilisateurs, etc.

34. Srnicek N., *Platform Capitalism*, Cambridge, Polity Press, 2017.

35. *Idem*.

La plateforme dominante en termes de revenus totaux issus de la publicité ciblée est Google, une entreprise fondée en 1996. Google a commencé par la collecte de données provenant des recherches d'utilisateurs afin d'optimiser les résultats de recherche. En 2000, l'entreprise a lancé AdWords et a commencé à vendre des espaces aux annonceurs pour une publicité ciblée à travers un système automatisé d'enchères. Les revenus ainsi générés à l'aide de ce service ont progressé de manière très significative : par exemple, en 2017, Google et ses nombreuses filiales (YouTube, Applied Semantics, DoubleClick, etc.) ont engrangé 95,38 milliards de dollars en recettes publicitaires sur un revenu total de 110,9 milliards (soit 86 %) ³⁶. Les revenus des autres plateformes de recherche sur internet sont nettement inférieurs, mais néanmoins substantiels. Ainsi, en 2016, Yahoo a enregistré des recettes publicitaires de 4,66 milliards de dollars, tandis que les recettes publicitaires de Bing au cours de la même année atteignaient 1,6 milliard de dollars. La part des profits provenant de la publicité ciblée est même plus importante dans le cas de Facebook qui, avec plus de 1,5 milliard d'abonnés, est devenu la plus grande entreprise de média au monde sans produire le moindre contenu original. En 2017, le réseau social a réalisé 39,94 milliards de dollars de recettes publicitaires, ce qui représente 98 % du revenu global de Facebook en 2017 ³⁷.

Le modèle commercial des plateformes de troc consiste à fournir un accès au marché basé sur le *cloud* aux acheteurs et vendeurs de produits. Dans le cas d'eBay, les revenus proviennent essentiellement des frais que la plateforme prélève sur chaque transaction, mais depuis quelques années, elle a également commencé à tirer des profits de la publicité ciblée. Ainsi, son chiffre d'affaires en 2017 s'élevait à 9,56 milliards de dollars, l'essentiel provenant toujours de ses frais de transaction mais les recettes publicitaires s'élevant déjà à 897 millions de dollars (9,3 % du total) ³⁸. En revanche, Taobao, l'équivalent chinois d'eBay, ne facture ni frais de vente ni frais d'insertion d'articles, et ne prélève pas de commission sur la vente. Ses revenus sont tous issus de la publicité ciblée.

La seconde catégorie – les plateformes en tant que moyens auxiliaires de production – comprend les plateformes qui fournissent des outils qui seront utilisés par d'autres. Ainsi, les produits créés requièrent des intrants et/ou des moyens de production additionnels. Elles sont bien plus nombreuses et opèrent dans une multitude de secteurs. Pour commencer, il y a ce que Srnicek appelle les « plateformes de *cloud* », à savoir celles qui offrent différents outils basés sur le *cloud* qui peuvent être employés par les utilisateurs afin de créer et commercialiser leurs propres produits ou services. À titre d'exemple, les développeurs peuvent utiliser l'écosystème Apple (XCode et le iOS SDK)

36. Voir statista.com

37. *Idem.*

38. *Idem.*

pour développer des applications et les vendre via l'App Store, Apple prélevant un pourcentage sur chaque vente. En d'autres termes, les développeurs utilisent leurs propres moyens de production (les ordinateurs) et leur capital humain (les connaissances en programmation) qui sont combinés aux outils fournis par les plateformes pour créer le produit final. Le même modèle est utilisé par Microsoft et Google qui offrent aux développeurs des outils similaires de création d'applications. Le lieu de vente des applications dépend de la plateforme dont les outils ont été choisis par le développeur (App Store si la plateforme choisie est Apple ; Google Play s'il s'agit d'outils basés sur Android de Google ou Microsoft App Store pour les outils Microsoft).

Nous pouvons également inclure dans cette catégorie les plateformes qui permettent aux prestataires de services de divers ordres de trouver des clients. L'un des principaux exemples ici est Uber, un service de taxi lancé à San Francisco en mars 2009. Cinq ans plus tard, il opérait dans plus de deux cents villes à l'échelle mondiale et était valorisé à plus de cinquante milliards de dollars, et ce sans posséder la moindre voiture. L'activité d'Uber se résume à produire *via* sa plateforme (en ayant recours aux données de circulation et aux situations géographiques des conducteurs et des passagers) des transactions entre les conducteurs, qui possèdent le moyen de production (les voitures et leur force de travail), et les passagers. Uber facture des frais aux conducteurs. Il en va de même pour Airbnb : dans ce cas, les fournisseurs de service (logement) possèdent les maisons et appartements qu'ils cèdent aux voyageurs et paient une redevance à Airbnb. Il existe aussi des plateformes qui aident des « entrepreneurs indépendants », à l'instar des *freelancers* ainsi que des prestataires proposant divers services tels que des travaux de réparation domestique ou de ménage, à trouver des clients. Ces entreprises sont désormais très nombreuses (TaskRabbit, UpWork, Workday, Elance...).

L'autre type de plateforme relevant de cette catégorie est Amazon Web Services (AWS), une plateforme fondée à l'origine pour la gestion de la logistique d'Amazon, mais qui est rapidement devenue un service informatique loué par cette dernière à d'autres utilisateurs, producteurs ou vendeurs qui ont besoin d'outils de développement de logiciels à la demande, de services pour les serveurs, d'espaces de stockage, de prestations informatiques, de systèmes d'exploitation ou encore d'applications prêtes à l'emploi. Comme le fait remarquer Srnicek, ce type de plateforme dispense les autres entreprises d'investir du temps et de l'argent dans la construction de leurs propres systèmes, matériels, kits de développement de logiciels ou applications. Elles peuvent se contenter de les louer lorsqu'elles en ont besoin. Le parallèle dressé entre ce service et la fourniture d'électricité par le PDG d'Amazon Jeff Bezos ³⁹ est tout à fait pertinent : tout comme l'électricité fournie à la demande a remplacé les générateurs individuels jadis employés par les usines, Amazon fournit dés-

39. Cité dans Srnicek N., *Platform Capitalism*, op. cit., p. 79.

ormais une infrastructure numérique dont les industries ont de plus en plus besoin à un certain stade de la production. En écho au succès d'Amazon dans ce domaine, (AWS a atteint une valeur estimative nette de près de soixante-dix milliards de dollars en 2015 ⁴⁰), Microsoft a également commencé à fournir aux autres entreprises une plateforme d'intelligence artificielle qui leur permet de créer leurs propres *bots* (« intelligence comme service ») ⁴¹, alors que Google s'essaye à vendre ses processus d'apprentissage automatique (*machine-learning processes*) basés sur le *cloud*. Le géant chinois Alibaba s'oriente également vers la fourniture de différents services similaires hébergés sur le *cloud*.

Enfin, nous pouvons ajouter à cette liste ce que Srnicek appelle les « plateformes industrielles » qui constituent le dernier développement dans le domaine des plateformes. Ici, les plateformes numériques commencent à participer aux procédés de production conventionnelle à travers l'installation de capteurs et traceurs dans différents composants ou intrants connectés à internet, procédé également connu sous les appellations « industrie 4.0 » ou « quatrième révolution industrielle » (après l'alimentation à la vapeur, l'électricité et les chaînes d'assemblage, et l'informatisation) ⁴². L'objectif des parties prenantes à l'industrie 4.0 est de créer des « usines intelligentes » (*smart factories*) fondées sur un système de partage en temps réel, par des composants individuels impliqués dans la production, d'informations sur leur localisation ou leur état, avec d'autres composants ou des ouvriers et cadres humains. L'une des premières plateformes construites pour l'industrie est MindSphere de Siemens, un système d'exploitation basé sur le *cloud* dont le développement a coûté quatre milliards de dollars à Siemens et qui connecte les produits, les usines, les systèmes et les machines. En plus de fournir ses propres applications, Siemens permet à des développeurs tiers de créer des applications et de les commercialiser via MindSphere (exactement de la même manière que l'App Store ou Google Play opèrent avec les développeurs d'applications). Un certain nombre d'applications de tiers sont déjà disponibles sur MindSphere, telles que Manufacturing Sustainability App et Production Confirmation App développées par Atos, Assembly Line Self Optimizing App d'Evosoft ou encore Connected Asset Management d'Accenture ⁴³. L'autre plateforme majeure de l'industrie 4.0 est Predix, qui a été créée par General Electric, et qui offre deux environnements de développement : un pour les développeurs hautement qualifiés qui peuvent accéder aux blocs de construction dans leur intégralité, et un pour les novices en codage qui peuvent profiter de l'environnement code du niveau inférieur, ainsi que de « Predix Studio » pour le dévelop-

40. Asay M., « Amazon's Cloud Business is Worth at least \$70 Billion », *ReadWrite*, 23 octobre 2015.

41. Un type de programme informatique qui effectue des tâches automatisées.

42. Marr B., « Why Everyone Must Get Ready for the 4th Industrial Revolution », *Forbes*, 5 avril 2016.

43. Voir siemens.com

pement rapide des applications ⁴⁴. En 2015, la Commission européenne a également lancé un projet de recherche (CREMA) sur l'industrie 4.0 dont l'objectif est de favoriser une production flexible et rapide basée sur le *cloud* et fondée sur les services informatiques EaaS (Everything as a Service) ainsi que sur l'utilisation innovante de l'intelligence artificielle et des technologies sémantiques. Le principal objectif de ce projet est d'aider l'industrie à améliorer son efficacité en matière de fabrication via le *leasing* sur demande et la fourniture de biens de fabrication selon une base de tarification à l'utilisation.

Surveillance : le moteur des plateformes numériques

Les différents types de plateformes numériques examinés partagent un élément central : ils impliquent tous la possession d'actifs immatériels (tels que les algorithmes ou les lignes de codes) associés à un capital physique souvent assez limité. De leur point de vue, le processus d'accumulation du capital est basé quasi exclusivement sur ce « nouveau pétrole » que sont les données, collectées, traitées, analysées puis monétisées sous différentes formes. Sans cette « matière première », leur modèle commercial ne peut exister. Dans le volume I du *Capital*, Marx faisait remarquer au sujet du capital qu'il ne naît que lorsqu'il rencontre sur le marché une « marchandise spécifique » – la force de travail ⁴⁵. Le capital, dit-il, « apparaît seulement là où le détenteur des moyens de production et de subsistance rencontre sur le marché le travailleur libre qui vient y vendre sa force de travail ⁴⁶ ». Nous pouvons paraphraser Marx en soutenant que le capital de plateforme requiert pour son apparition une marchandise très spécifique : les données, et surtout celles de l'utilisateur. Elle peut être ajoutée à la liste des trois « marchandises fictives » de Karl Polanyi, définies comme des marchandises qui ne sont pas initialement produites pour la vente, mais qui sont objectifiées dans le capitalisme ⁴⁷. Les données utilisateur sont peut-être la marchandise la plus fictive, car non seulement elles ne sont pas produites pour la vente par les utilisateurs (qui naviguent simplement sur internet ou partagent du contenu avec des amis sur les réseaux sociaux), mais elles sont également les plus immatérielles de toutes : il s'agit d'une marchandise fictive basée sur le *cloud*. Ainsi, il existe désormais de nombreuses entreprises générant des milliards de dollars de profits et opérant dans un nombre croissant de secteurs dont la capacité même à générer ces profits dépend entièrement de la surveillance des utilisateurs individuels et, de plus en plus, des objets matériels. Examinons maintenant cette question dans le détail, en particulier sous le prisme de la surveillance des utilisateurs individuels.

44. Voir ge.com.

45. Marx K., *Capital: Critique of Political Economy*, Volume I, Londres, Penguin Books, 1976, p. 270.

46. *Ibid.*, p. 274.

47. Polanyi K., *The Great Transformation: The Political and Economic Origins of Our Time*, *op. cit.*

La question de l'acquisition des données est bien évidemment vitale pour les plateformes opérant en tant que facteurs de production à part entière. Il s'agit ici de leur « matière première », de ce dont elles ont besoin pour générer des revenus, ce qui explique le volume des données utilisateurs qu'elles collectent. Ainsi, Google recueille les données utilisateurs suivantes : localisation du *smartphone* de l'utilisateur dès le premier jour où il s'y connecte à Google ; historique de recherche sur l'ensemble des appareils de l'utilisateur (conservé par Google, même si l'utilisateur le supprime sur ses appareils) ; informations sur toutes les applications et extensions utilisées (lieu et fréquence d'utilisation, personnes ou entités avec lesquelles il a été en communication à l'aide de l'application, etc.) ; intégralité de l'historique YouTube de l'utilisateur ; tous les marque-pages, mails, contacts, fichiers Google Drive, produits achetés *via* Google, etc. Enfin, de nombreuses autres informations sont collectées (la musique écoutée, les photos prises, les livres achetés, les téléphones possédés, les pages partagées, le nombre de pas effectués par jour, etc.). Le volume de données collecté par Facebook est également impressionnant : chaque message ou fichier envoyé ou reçu par l'utilisateur ; tous les contacts dans le téléphone de l'utilisateur ; les pages ou médias « likés », commentés et partagés ; chaque connexion à Facebook (le lieu à partir duquel l'utilisateur s'est connecté, l'heure et le type d'appareil à partir duquel la connexion a été effectuée) ; toutes les vignettes envoyées sur Facebook et toutes les applications connectées au compte Facebook de l'utilisateur.

À l'instar des industries traditionnelles qui ont besoin de plus de matières premières pour accroître leur production, ce type de plateforme a besoin de plus de données pour croître : la nécessité perpétuelle d'augmentation du volume d'acquisition des données est inhérente à ce modèle commercial. Des plateformes telles que Google et Facebook répondent à cette nécessité en augmentant leur capacité de collecte des données à la fois en termes de champ et de profondeur. Le premier aspect implique l'augmentation du nombre des sources à partir desquelles les données sont exploitées : l'acquisition d'autres entreprises ou startups prometteuses, la création de liens vers d'autres bases de données et réseaux. Facebook, par exemple, a élargi l'ampleur de ses capacités d'exploitation de données en rachetant des entreprises comme Instagram et WhatsApp, et en combinant les données obtenues par ses propres moyens aux informations recueillies par divers courtiers en données. Ainsi, Facebook a collaboré pendant plusieurs années avec des courtiers en données tels que Acxiom et Experian afin de créer de meilleures cibles publicitaires pour certaines catégories d'annonceurs (constructeurs automobiles, fabricants de produits de luxe et de produits de grande consommation qui ne vendent pas directement aux consommateurs et ont relativement peu d'informations sur leurs clients ⁴⁸). Google a également racheté des entreprises telles que

48. Reuters, « Facebook Cuts Ties to Data Brokers in Blow to Targeted Ads », *Business News*, 28 mars 2018.

YouTube, DoubleClick, AdMob, HTC afin d'augmenter le nombre de sources d'obtention de données. Concernant la profondeur d'acquisition des données, il s'agit de développer de nouveaux outils permettant d'en savoir plus sur les utilisateurs de la plateforme existante (par exemple, capacité améliorée de géolocalisation des utilisateurs, d'optimisation des méthodes d'analyse de leurs activités en ligne, *via* notamment le calcul du temps qu'ils passent à la consultation de certains types de contenu, le nombre de consultations par jour, etc.). Enfin, les plateformes ont besoin d'améliorer constamment leurs outils d'analyse (les algorithmes) des données obtenues afin d'élaborer des profils et segments d'utilisateurs plus nuancés pour pouvoir offrir de meilleurs produits finaux aux annonceurs, ces derniers cherchant à augmenter leur « taux de conversion » (*conversion rate*), c'est-à-dire le pourcentage d'utilisateurs qui finissent par acheter leurs produits ou services grâce aux publicités placées sur ces plateformes numériques. Ainsi, Google modifie son algorithme de recherche cinq à six cents fois par an afin d'améliorer ses capacités d'analyse des données et de fournir de meilleurs résultats de recherche. La plupart de ces changements sont généralement mineurs, mais Google introduit de temps en temps d'importantes mises à jour algorithmiques (telles que Google Panda et Google Penguin).

S'agissant des plateformes qui fonctionnent en tant que moyens auxiliaires de production, leur degré de dépendance aux données peut varier, mais elles sont toutes également soumises à l'impératif d'améliorer constamment leur capacité de collecte et d'analyse des données. Par exemple, les plateformes qui fournissent des outils et l'accès au marché permettant aux développeurs de créer et de vendre les applications (Google Play, Microsoft App Store ou Apple App Store) doivent en savoir toujours plus sur les clients qui achètent un type spécifique d'applications afin d'optimiser leurs méthodes de publicité ciblée et, par ce biais, augmenter les ventes d'applications sur lesquelles elles chargent une commission. Les boutiques en ligne telles que Amazon ou Alibaba, ou les plateformes de troc comme eBay ou Taobao, obéissent au même impératif. Les plateformes comme Uber, ou celles qui mettent en contact les « entrepreneurs indépendants » et les clients, doivent également en savoir le plus possible sur la qualité des services fournis par les prestataires (des conducteurs, des nettoyeurs, des réparateurs, etc.). Pour ce faire, des techniques plus sophistiquées de traçage des conducteurs, par exemple, sont développées (ainsi, Uber suit désormais en permanence la position des conducteurs afin de minimiser les délais d'attente pour les clients) et la performance de chaque prestataire est sans cesse notée et évaluée.

Ces impératifs sont peut-être moins prononcés dans le cas des plateformes industrielles, mais n'oublions pas que l'objectif de l'industrie 4.0 ne consiste pas uniquement à intégrer des systèmes de communication en temps réel aux composants du processus de production, mais aussi à les établir entre les

objets et les travailleurs humains. Ceci crée une incitation à équiper également les ouvriers de capteurs et autres appareils électroniques permettant une évaluation de leurs performances. En réalité, ce type de dispositifs de surveillance et de traçage des employés est déjà largement utilisé dans différents secteurs. Ainsi, des entreprises telles que Sociometric Solutions ont développé des badges d'identification d'employés (équipés d'un microphone, d'un capteur de position et d'un accéléromètre) pour mieux connaître la « dynamique sociale » (*social dynamics*) parmi les salariés : à qui parlent les employés, sur quel ton, pendant quelle durée, etc.⁴⁹. Des techniques de surveillance similaires sont maintenant proposées par de nombreuses autres entreprises (InterGuard, ObserveIt, Steelcase, Epicenter, etc.). Epicenter est allé jusqu'à développer des micropuces implantées sous la peau des employés, afin non seulement de les surveiller, mais aussi de leur donner la possibilité d'ouvrir des portes à distance, d'acheter des en-cas à partir de distributeurs automatiques ou encore de faire fonctionner des imprimantes (ce qui permet, par la même occasion, d'élargir le champ des connaissances dont dispose la direction sur chaque employé). Plus récemment, Amazon a déposé un brevet pour un bracelet numérique qui suit les mouvements des ouvriers au sein de ses entrepôts et peut vibrer pour orienter les employés dans la bonne direction⁵⁰. À l'aune de ces évolutions, il est plausible de supposer que ce type de dispositifs sera, tôt ou tard, utilisé par les plateformes de l'industrie 4.0 et qu'un volume accru de données personnelles des employés sera ainsi exploité et analysé.

Néanmoins, l'un des principaux obstacles auxquels sont aujourd'hui confrontées les plateformes numériques dans leurs tentatives d'acquérir une plus grande quantité de « matières premières », c'est-à-dire de savoir sur les utilisateurs, les employés et les « entrepreneurs indépendants », est le droit au respect de la vie privée, consacré dans les différents instruments juridiques nationaux et internationaux. Le principal moyen utilisé par les plateformes pour contourner cet obstacle est d'obtenir le consentement de l'utilisateur – son acceptation des conditions d'utilisation des services proposés. Toutefois, les utilisateurs sont-ils réellement conscients de ce à quoi ils donnent leur consentement ? Il ne serait pas exagéré de soutenir que ce n'est pas le cas pour la vaste majorité des utilisateurs, dans la mesure où les conditions d'utilisation, en règle générale, se caractérisent par une très grande complexité, une incompréhensibilité et une longueur déraisonnable, les dispositions concernant le consentement de l'utilisateur à la collecte et à l'analyse des données utilisateur et à leur partage avec des tiers étant extrêmement difficiles à identifier et à comprendre. Par exemple, il a fallu huit heures et cinquante-neuf minutes à un acteur recruté par l'association des consommateurs Choice pour lire les 73 198

49. Manokha I., « Why the Rise of Wearable Tech to Monitor Employees Is Worrying », *The Conversation*, 3 janvier 2017.

50. « Amazon Patents Wristband that Tracks Warehouse Workers' Movements », *The Guardian*, 1^{er} février 2018.

mots des conditions d'utilisation d'Amazon Kindle ⁵¹. En outre, dans des cas où il est possible de désactiver certaines fonctionnalités afin d'améliorer la protection des données personnelles, lors de l'installation ou de l'inscription initiale, celles-ci sont activées par défaut et il est souvent également fastidieux de les désactiver. À titre d'exemple, le système d'exploitation Windows 10 de Microsoft compte seize sous-menus distincts dans la rubrique « Options de confidentialité » (localisation, programmes installés et toutes les informations concernant leur utilisation, accès à la webcam et au microphone, accès aux contacts, messages électroniques, calendrier, fichiers téléchargés, photos et vidéos, musique, historique de recherche et de navigation). Facebook continue à collecter des données sur les utilisateurs lorsqu'ils sont déconnectés, grâce aux boutons « Like » et à l'outil de connexion de Facebook ⁵². L'utilisation de toutes ces astuces par les différentes plateformes ne peut être comprise que si l'on saisit la nature de leur modèle commercial qui les incite, voire les oblige, à inventer les différentes méthodes de contournement des obstacles susceptibles de les empêcher d'obtenir davantage de données.

À cet égard, nous pouvons constater que la différence entre les méthodes des plateformes numériques et celles auxquelles a eu recours Cambridge Analytica n'est pas très significative. Cependant, seules ces dernières, qui sont considérées comme illégales, suscitent une indignation générale, alors que les données ainsi collectées ne représentent qu'une goutte d'eau en comparaison du volume d'informations que le capital de plateforme recueille sans cesse. Ainsi, même si le tollé général visant Cambridge Analytica a fini par conduire à sa fermeture, il s'agit d'une victoire à la Pyrrhus ⁵³ dans la mesure où l'existence des plateformes possédant des quantités gigantesques d'informations sur les goûts, intérêts, convictions politiques, habitudes, voyages, etc., de millions d'utilisateurs n'a pas du tout été mise en cause, et où la monétisation incessante des données privées se poursuit. On peut donc soutenir que le capital de plateforme constitue aujourd'hui, avec les différentes autorités publiques (notamment celles en charge des questions de sécurité), l'une de forces les plus puissantes ⁵⁴ contribuant à l'affaiblissement du droit à la vie privée. Or,

51. Choice, « How Long Does It Take to Read Amazon Kindle's Terms and Conditions? », YouTube, 17 mars 2017, en ligne sur <https://www.youtube.com/watch?v=sxygkyskucA>, consulté le 01/04/2018.

52. Nieva R., « Here's How Facebook Collects Your Data When You're Logged Out », *CNET*, 16 avril 2018.

53. Manokha I., « Cambridge Analytica's Closure is a Pyrrhic Victory for Data Privacy », *The Conversation*, 3 mai 2018, en ligne sur <https://theconversation.com/cambridge-analyticas-closure-is-a-pyrrhic-victory-for-data-privacy-96034>, consulté le 13/05/2018.

54. Il convient également de mentionner ici d'autres acteurs dont l'impact sur le droit à la vie privée n'est, pour le moment, pas comparable à celui des plateformes numériques, mais qui possèdent des quantités de données de plus en plus importantes, tels que les courtiers en données et les sociétés de conseil utilisant les données personnelles dans leur activités commerciales (telles que i360, Data Trust, etc.). À titre d'exemple, Data Trust est actuellement en mesure de recueillir plus de 1 800 informations sur un individu, y compris des informations telles que le dernier film pornographique visionné ou le dernier plat chinois commandé (voir Palast, G.,

comme cela a été souligné par un grand nombre d'auteurs ⁵⁵, le droit à la vie privée est l'un des droits humains les plus fondamentaux, dans la mesure où sa violation porte non seulement atteinte à la dignité humaine mais peut également compromettre l'exercice de plusieurs autres libertés individuelles, telles que la liberté d'expression, d'information et de la presse, la liberté de pensée, de conscience et de religion, la liberté de réunion, d'association et de rassemblement pacifique, ainsi que certains droits des travailleurs. C'est pour cette raison que le non-respect croissant du droit à la vie privée, particulièrement dans les sociétés occidentales, a été désigné par Giorgio Agamben ⁵⁶ comme étant l'une des principales menaces à l'existence même de la politique dans les sociétés démocratiques actuelles.

En somme, tant que les plateformes perdureront, les invasions régulières de la sphère privée, indispensables au fonctionnement du capital de plateforme subsisteront, et l'idée selon laquelle les données sont une marchandise dont la possession peut générer des revenus deviendra de plus en plus objectivée et normalisée.

Cette analyse nous permet de tirer un certain nombre de conclusions générales. Rappelons tout d'abord que la phase actuelle de développement du capitalisme ne saurait être désignée selon nous ni comme un « capitalisme de surveillance », ni comme un « capitalisme de plateforme ». La thèse développée ici est que le capitalisme moderne se caractérise par l'importance grandissante du capital de plateforme, qui est un type de capital singulier dans la mesure où sa reproduction et sa valorisation reposent sur une « matière première » particulière, immatérielle : les données, et notamment les données utilisateur. En d'autres termes, les données constituent la marchandise que le capital de plateforme doit nécessairement rencontrer sur le marché afin de devenir capital, pour paraphraser Marx une fois de plus. Cela signifie que la

« Cambridge Analytica is Not Alone: i360 and Data Trust Disastrous for Democracy », TheRealNews.com, 29 mars 2018).

55. Voir notamment les travaux classiques de Westin A., *Privacy and Freedom*, New York, Atheneum, 1967 et de Rule J., *Private Lives and Public Surveillance: Social Control in the Computer Age*, Londres, Allen Lane, 1973, ainsi que les travaux plus récents tels que Bauman Z. et al., « After Snowden: Rethinking the Impact of Surveillance », *International Political Sociology*, vol. 8, n° 2, 2014, pp. 121-144 ; Bennett C., « Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications », *Surveillance & Society*, vol. 13, n° 3/4, 2015, pp. 370-384 ; Ball K., « Workplace Surveillance: an Overview », *Labour History*, vol. 51, n° 1, 2010, pp. 87-106 ; Boghosian H., *Spying on Democracy: Government Surveillance, Corporate Power, and Public Resistance*, San Francisco, City Lights Books 2013 ; Manokha I., « Why the Rise of Wearable Tech to Monitor Employees Is Worrying », art. cit., Foer, F., *World Without Mind: The Existential Threat of Big Data*, New York, Penguin Press, 2017.
56. Agamben G., « From the State of Control to the Praxis of Destituent Power », 4 février 2014, en ligne sur <https://roarmag.org/essays/agamben-destituent-power-democracy/>, consulté le 13/05/2018.

surveillance, la collecte et le traitement des données personnelles (y compris, de plus en plus, des données concernant les objets matériels) – constituent des instruments indispensables aux plateformes, ainsi qu’aux autres entités commerciales monétisant les données, pour créer de la valeur. Cet impératif est particulièrement prononcé pour les types de plateforme qui fonctionnent comme moyens de production à part entière (tels que les moteurs de recherche internet) ou les réseaux sociaux qui utilisent des facteurs de production essentiellement immatériels (algorithmes) et se servent des données comme « matière première » unique pour générer les revenus. Nous avons également constaté que les plateformes qui jouent le rôle de moyens de production auxiliaires sont aussi confrontées à la nécessité d’améliorer en permanence leurs capacités de collecte et traitement des données, même si cet impératif est parfois moins prononcé dans leur cas.

Dans ce contexte, les données sont devenues une marchandise : elles peuvent désormais être achetées et monétisées, d’une manière ou d’une autre, afin de générer un profit. Nous avons affaire ici à un nouveau type de « marchandise fictive », qui semble être la plus fictive de toutes : non seulement elle n’est pas produite pour la vente (les utilisateurs naviguant et discutant sur la toile ne cherchent pas, par ce biais, à générer les données afin de les vendre), mais elle est totalement immatérielle de surcroît (n’étant, en réalité, qu’un ensemble de lignes de codes).

Concernant l’affaire Cambridge Analytica, l’objectif principal du présent article a été de montrer qu’il ne s’agissait que de la partie émergée de l’iceberg. Le volume de données acquises par cette société de conseil est dérisoire par rapport à celui de géants comme Google et Facebook, ainsi que d’autres types de plateformes susmentionnés, qui collectent, analysent et monétisent de manière constante des données sur les individus sans qu’ils en aient réellement conscience. En effet, la seule différence entre cette collecte régulière des données et Cambridge Analytica est que cette dernière a utilisé des moyens plus dissimulés pour accéder à ces données. À cet égard, nous pouvons soutenir que les mobilisations contre Cambridge Analytica et sa chute ultime sous la pression de différents acteurs ont trois implications : premièrement, ceux qui ont ciblé cette société de conseil ont uniquement mis en cause des mesures de collecte « clandestines » de données et, de ce fait, ont involontairement contribué à la normalisation de celles qui sont, de façon générale, considérées comme étant légitimes (celles auxquelles les utilisateurs donnent leur consentement en acceptant les différentes conditions d’utilisation) ; deuxièmement, dans la mesure où les mobilisations contre Cambridge Analytica n’ont pas contesté l’existence et l’activité des plateformes numériques, les conditions structurelles incitant certaines entités à commettre ce type d’action afin d’accéder aux données détenues par des plateformes continueront d’exister, et des scandales similaires (impliquant des acteurs publics ou privés) sont suscepti-

bles de se reproduire ; troisièmement, même si le tollé général a abouti à la chute de Cambridge Analytica, d'autres acteurs similaires, notamment des sociétés de conseil ou des courtiers en données, continueront à collaborer avec des plateformes numériques et détiendront de plus en plus de données.

Enfin, les protestataires invoquent souvent le droit au respect de la vie privée pour condamner différents cas de collecte de données personnelles. Toutefois, d'une part, certains de ces lanceurs d'alerte, l'*Observer* et le *New York Times* qui ont révélé le vol de données par Cambridge Analytica, sont eux-mêmes impliqués dans la collecte de données pour des tiers, ce qui contribue au processus de marchandisation des données et, par ailleurs, soulève des questions sur leur conception du respect de la vie privée. D'autre part, compte tenu de la puissance financière des plateformes numériques, il semble très peu probable que les acteurs qui militent actuellement pour une meilleure protection des données personnelles par les plateformes (et notamment par Facebook, à la suite du vol commis par Cambridge Analytica) en évoquant le droit à la vie privée, aboutissent à des changements significatifs dans ce domaine. En effet, l'invasion perpétuelle de la sphère privée est tout simplement indispensable pour la reproduction du capital de plateforme. De plus, du fait de la part croissante du capital de plateforme dans le capitalisme actuel, enrayer son fonctionnement aurait inévitablement un impact négatif sur la croissance économique. Par exemple, les règles de protection de la sphère privée sont bien plus strictes dans l'UE qu'aux États-Unis. Conséquence : le nombre de « startups valorisées à un milliard de dollars est de quarante-deux aux États-Unis et de treize seulement dans l'UE » et « des données récentes suggèrent que le régime de protection des données de l'UE a déjà eu un impact notable sur l'économie ⁵⁷ ». Dans ce contexte, on peut également s'attendre à l'émergence d'opposants au renforcement des mesures de protection de la vie privée pour ces raisons. En résumé, si les citoyens souhaitent reprendre le contrôle de données relatives à leurs vies privées, ils doivent s'organiser afin de défier le capital de plateforme dans son ensemble et pas seulement des acteurs isolés comme Cambridge Analytica.

57. Parker G., Van Alstyne M. et S. Choudary, *Platform Revolution: How Networked Markets Are Transforming The Economy - And How To Make Them Work For You*, New York, W.W. Norton & Company, 2016. Voir également Goldfarb A. et C. Tucker, « Privacy Regulation and Online Advertising », *Management Science*, vol. 57, n° 1, 2011, pp. 57-71.